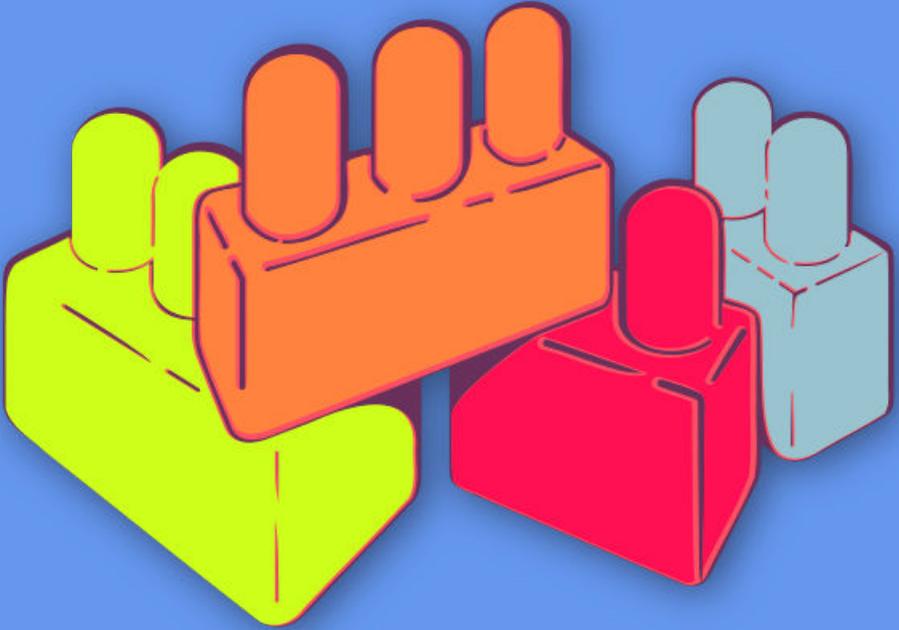




النساء فى فضاء الإنترنت



أسس الأمن الرقمي | الجولة
الثانية

لنعد إلى خانة الصفر (إعادة الضبط)!

**INSTITUTE FOR
WAR & PEACE REPORTING**



© 2019– Institute For War And Peace Reporting

<https://iwpr.net/>



نَسَبُ الْمُصَنَّفِ - الترخيص بالمثل 4.0 دولي

<https://creativecommons.org/licenses/by-sa/4.0/deed.ar>

المحتويات

٥	١ نعد إلى خانة الصفر (إعادة الضبط)!
٦	إدارة الجلسة
٦	الجزء الأول - تبيد الخرافات
٧	الجزء الثاني - ما الذي نعنيه فعليا بإعادة الضبط؟
٨	الجزء الثالث - التحقق: هل تحتجن لإنشاء نسخ إحتياطية؟
٨	الجزء الرابع - إعادة الضبط وإعادة التشغيل Resetting & Rebooting
٩	الجزء الخامس - الأنظمة التشغيلية الحية
١١	الجزء السادس - الممارسة التطبيقية
١٢	المراجع

باب ١

لنعد إلى خانة الصفر (إعادة الضبط)!

- الأهداف: تعزز هذه الجلسة فكرة أنه "ليس للأدوات والتكنولوجيا سطوة سحرية خارقة علينا!" ستقدن المشاركات هنا في عملية سترفع من مستوى قدراتهن هي عملية "البدء من خانة الصفر" عبر إعادة ضبط أجهزتهن من أجل البدء باستخدامها وكأنها جديدة.
- الطول: 90 دقيقة
- الشكل: جلسة
- مستوى المهارة: متوسط
- المعرفة المطلوبة:
- معرفة مفاهيم الأمن الرقمي الأساسية و/أو تدريب مسبق
- تعريف بمسألة التشفير (التشفير)
- التخزين والتشفير (أسس الأمن الرقمي، الجولة الثانية)
- جلسات/تمارين ذات صلة:
- وجهات النظر الشخصية حيال الأمن^١
- البرمجيات الخبيثة والفيروسات^٢

^١<https://vrr.im/9339>

^٢<https://vrr.im/47e5>

- الخوصية^٣
- المزيد من الهويات الإلكترونية!^٤
- التخزين والتشفير^٥
- المواد اللازمة:
 - شراخ (فيها النقاط المفتاحية الواردة أدناه)
 - مفاتيح يو إس بي مجهزة بنظامي تايلز وأوبونتو Ubuntu القابلين لإعادة التشغيل.
 - التوصيات: فكرن في جلب مفاتيح يو إس بي مجهزة بنظام تشغيل لكل مشاركة على أن يحتفظن بها؛ والأجهزة حاسوباً لتتدرب المشاركات عليه (أو إثين في حال عرضتن نظامي تايلز وأوبونتو التشغيليين) - وحتى لو كان الهدف من النشاط تشغيل نظامي تايلز أو أوبونتو من مفتاح يو إس بي مجهزة بنظام تشغيل، عوضاً عن تثبيتته، قد لا تشعر بعض المشاركات بالإرتياح لإستعمال حاسوبهن الخاص لإختباره. من الممكن أيضاً تغيير ذلك بحيث يسهل إدخاله إلى أي جلسة مخصصة لانشاطات لا يخن من شيء في ورشتكن التدريبية، يرغن في تغيير الأنظمة التشغيلية بالكامل من ماك أو ويندوز إلى نظام كنظام أوبونتو من شركة لينوكس linux.

إدارة الجلسة

الجزء الأول - تبديد الخرافات

الجزء الأول - تبديد الخرافات

١. إبدأن الجلسة بشرح الهدف من هذه الجلسة: إعادة تأكيد قدرة الإنسان على التحكم بالتكنولوجيا، وتبديد فكرة أن الأجهزة الرقمية لها "قوى خارقة" تسيطر من خلالها على مستخدميه. في حال قدمتن جلسة وجهات النظر الشخصية حيال الأمن للمشاركات، يمكنكن تذكيرهن بما يلي من التأكيدات الختامية:

<https://vrr.im/819e٣>

<https://vrr.im/e9f7٤>

<https://vrr.im/0ccc٥>

ليس للأدوات والتكنولوجيا سطوة سحرية خارقة علينا! نحن من يقرر ما يمكنها الوصول إليه، وفي حال طرأ أي حادث، يمكننا دوماً إعادة ضبطها!

الجزء الثاني - ما الذي نعينه فعلياً بإعادة الضبط؟

٢. كررنا للمجموعة هذا التأكيد من المرحلة السابقة، وشددنا على الجملة الأخيرة منه "يمكننا دوماً إعادة ضبطها" - ماذا يعني ذلك؟ إشرح لنا ذلك عبر تقديم السيناريو التالي: لعلك في إحدى محطات مسيرتك مع الأمن الرقمي، شعرت أنك تقمن بكل شيء بالطريقة الخاطئة.

تنظرن إلى حاسوبكن - هو مليء بالبرمجيات المقرصنة والأفلام والبرامج التلفزيونية المنزلة عبر منصة "تورينت" والملفات الأخرى المبعثرة التي لا تتذكرن حتى أنك نزلتتها. استخدمتن مفاتيح اليو إس بي من دون تمييز - على حاسوبكن المحمول، وعلى حواسيب وآلات طباعة في مقاهي إنترنت، وربما لا تقمن دائماً بإخراجها بالطريقة الصحيحة حين تنتهين من استخدامها.

ربما انفصلتن مؤخراً عن شخص ما تعرفن جيداً أنه/ها كان يفتح حاسوبكن في غيابكن - وربما قام/ت بتخمين كلمة السر أو حتى أعطيته/ها إياها بأنفسكن.

والآن، تشعرن بأنكن فقدتن السيطرة - من يعرف ما نوع الفيروسات الموجودة على قرصكن الصلب، أو من ياترى له القدرة على الوصول إلى معلوماتكن؟ ولكن على فكرة، ذلك ليس مشكلة كبيرة! لم يفث الأوان بعد لفتح صفحة جديدة. هل ترغبن في فتح صفحة جديدة؟ هذه الجلسة معدة خصيصاً لكنّ إذا!

٣. والآن، بعد أن قرأتن السيناريو الوارد أعلاه لتحديد السياق، يمكنكن شرح ما يعني مصطلح إعادة الضبط في هذا السياق: أي البدء من خانة الصفر عبر إعادة ضبط جهازكن أو حاسوبكن إلى حالته وإعداداته الأصلية، وبالتالي منح أنفسكن "صفحة بيضاء" لمسيرة الأمن الرقمي الخاصة بكن.

لا تسين تذكير المشاركات أن هذه الجلسة ستفسّر لمن كيفية إجراء عملية إعادة ضبط - لن يتوجب عليهن إجراء عملية إعادة ضبط خلال الجلسة، أو حتى خلال التمرين. فقد تترتب نتائج سيئة جداً عن عملية إعادة الضبط في حال لم تكن المشاركات جاهزات لها، أو في حال لم يقمن بإجراء نسخ احتياطية لبياناتهن مؤخراً - وقد يحتجن لحواسيبهن المحمولة بما أنهن يرغبن حالياً بالمحافظة على قدرتهن على الوصول إلى بياناتهن إلى أن يصبحن جاهزات أكثر لإجراء عملية إعادة الضبط. ولكن، خلال هذه الجلسة ستتاح للمشاركات فرصة التدرّب بواسطة أنظمة تشغيل بديلة على حواسيبهن، وهذا ما يشكل محطة تحضيرية مهمة في حال قررن إجراء عملية إعادة ضبط لاحقاً.

الجزء الثالث - التحقق: هل تحتجن لإنشاء نسخ احتياطية؟

٤. يفصّل أن تكنّ قد قدمتن قبل الآن جلسة التخزين والتشفير للمشاركات بما أنها تناولن نقاطاً مهمة في مجال إنشاء نسخ احتياطية للبيانات. بكل الأحوال، قبل أن تبدأن بالجزء الخاص بالممارسة التطبيقية من هذه الجلسة، قمن بعملية تحقق سريعة مع المجموعة حول إنشاء نسخ احتياطية لبياناتهن.

إختياري: كتذكير سريع بجلسة التخزين والتشفير، إسألن المشاركات - كم مرّة في السنة يقمن بنسخ احتياطي لملفاتهن؟ شاركن أمثلة عن الممارسات الفضلى في مجال إنشاء نسخ احتياطية للبيانات، من قبيل الإحتفاظ بالنسخة الإحتياطية في مكان آمن منفصل عن حاسوبهن، وإنشاء نسخ احتياطية لمعلوماتهن بشكل دوري ومتكرر، بحسب المعلومات التي ينشأ لها نسخ احتياطية، والتفكير أيضاً في تشفير القرص الصلب أو وسيط التخزين حيث سيقمن بتخزين البيانات.

الجزء الرابع - إعادة الضبط وإعادة التشغيل Resetting & Rebooting

٥. قبل البدء بالجزء الخاص بالممارسة التطبيقية من هذه الجلسة، لا بد من تناول مسألة مهمة هي العلاقة بين إعادة التشغيل وإعادة الضبط فرمما إستخدم هذان المصطلحان من

دون تمييز بينهما طوال هذه الجلسة:

يدلّ هذان المصطلحان إلى عمليتين تشبه بعضهما إلى حد كبير بالمعنى العام، ولكن ذكرن المشاركات أن كلمة "إعادة الضبط" تستخدم هنا للدلالة على مفهوم "فتح صفحة جديدة" في سياق هذه الجلسة. عملية إعادة التشغيل هي عملية تقنية تجريها حواسيبهن خلال عملية إعادة فتحها؛ هي عملية مهمة أيضاً يجب فهمها من أجل الممارسة التطبيقية لأنظمة التشغيل البديلة التي ستجرى في الجزء التالي من الجلسة.

٠٦. لمزيد من التوضيح للفكرة الواردة أعلاه، قدمنا أنظمة تشغيل تايلز وأوبونتو إلى جانب تقديم بعض المعلومات التقنية القيّمة للمشاركات التي ستكون مفيدة في الجزء التالي من الجلسة. إشرحن ما الذي يجعل من تايلز وأوبونتو نظامين بديلين عن أنظمة التشغيل الأخرى مثل ماك أو إس وويندوز - في هذه الجلسة، سيركز الجزء الخاص بالممارسة التطبيقية على تشغيل هذين النظامين التشغيليين من مفتاح يو إس بي.

الجزء الخامس - الأنظمة التشغيلية الحية

٠٧. قد يطرح عليكم سؤالاً من قبيل: كيف يمكننا استخدام النظام التشغيلي الجديد على حواسيبنا المحمولة من دون التخلّص من الذي نستخدمه الآن؟ ماذا سيحدث لبياناتنا؟ عليكم الآن إغتنام هذه الفرصة لشرح بعض المصطلحات للمشاركات قد تساعدهن على فهم كيفية عمل تايلز وأوبونتو في سياق هذه الجلسة بشكلٍ أوضح:

النظام الحي Live System

النظام الحيّ هو نظام تشغيلي يمكن تشغيله مباشرة من وسيط تخزين خارجي مثل مفتاح يو إس بي أو شريحة ذاكرة. نظام تايلز التشغيلي هو مثال عن الأنظمة الحية؛ ومن الممكن إعداد أوبونتو للعمل كنظام حيّ، وهو "نسخة" أخرى عن النظام التشغيلي المستند إلى نظام لينوكس الذي يستعين به نظام تايلز.

لينوكس Linux

لينوكس نظام تشغيلي شبيه بنظامي ويندوز وماك، إلا أن الفرق الرئيسي بينه وبينهما هو أنه موزع كبرمجية مجانية ومفتوحة المصدر. ولذلك، تتوفر نسخ مختلفة كثيرة مستندة إلى نظام لينوكس - نظام دبيان Debian، هو إحدى النسخ الأكثر شعبية وهو يشكل أساس نظام تايلز.

الجهاز القابل للتشغيل Bootable Device

أجهزة التشغيل (أو القابلة للتشغيل) هو جهاز أو قرص يمكن للحاسوب تحميل ملفات منه للتمكن من العمل. على سبيل المثال، على معظم الحواسيب يعتبر القرص الصلب جهاز التشغيل الذي يتم من خلاله تحميل نظام التشغيل (مثل ويندوز) عند تشغيل الحاسوب. بالإضافة إلى الأقراص الصلبة، تعتبر الوسائط كالأقراص المدمجة CD وأقراص دي دي DVD وشرائح الذاكرة ومفاتيح اليو إس بي من الأجهزة القابلة للتشغيل.

نظام الإدخال والإخراج الأساسي (Basic Input/Output System Bios)

نظام الإدخال والإخراج الأساسي BIOS هو البرمجية الأولى التي تشغيلها معظم الحواسيب حيث يتم تشغيلها. يستخدم هذا النظام لإجراء عمليات إختبار ذاتية على الأنظمة والأجهزة لضمان عملها بشكل سليم، ومن أجل تفعيل تسلسل التحميل للبرمجيات (كالأنظمة التشغيلية) الموجودة على الأجهزة القابلة للتشغيل المتوفرة. يتمتع نظام الإدخال والإخراج بواجهة تفاعلية، ولكن لا يمكن للمستخدمين الوصول إليها إلا إذا قاموا بخطوة محددة خلال إقلاع الجهاز للوصول إليه مباشرة.

تسلسل التشغيل

تسلسل التشغيل، الذي يمكن الوصول إليه من خلال نظام الإدخال والإخراج (أو واجهة البرنامج الثابت الممتد UEFI) أثناء إقلاع حاسوب ما، هو لائحة بالأجهزة القابلة للتشغيل على حاسوب ما - يستخدم لتحديد التسلسل الذي يحاول الحاسوب وفقه تحميل المعلومات من هذه الأجهزة. عادةً القرص الصلب في الحاسوب هو الجهاز الأول في تسلسل التشغيل، ومنه يتم تحميل نظام التشغيل. ولكن من الممكن تغيير تسلسل التشغيل ليحمل معلومات من أجهزة خارجية قابلة للإزالة أولاً كأقرص دي في دي أو مفاتيح اليو إس بي.

الجزء السادس - الممارسة التطبيقية

٨. للبدء بالجزء المخصص للممارسة التطبيقية من هذه الجلسة، قسمن المشاركون إلى مجموعتين على الأقل. قدمن لكل مجموعة حاسوباً ليجرن عليه تشغيل نظام أوبونتو أو تايلز من مفتاح يو إس بي معدّ مسبقاً؛ أو، في حال توفر لديكن العدد الكافي من مفاتيح اليو إس بي المعدة مسبقاً لكل المشاركين، عندها سيتمكن من التدرّب كل واحدة على حدة (في هذه الحالة، ستقمن بجعل الجميع يتدربن على إستخدام إما نظام تايلز وإما نظام أوبونتو)

٩. على حاسوبكن المحمول، وبواسطة جهاز عرض، وجهن المشاركون عند إجرائهن لعملية إعادة تشغيل حواسيبهن وإطلاق نظام تايلز/أوبونتو خلال تسلسل تشغيل نظام الإدخال والإخراج. وأثناء قيامكن بذلك، إحرصن على شرح الفوارق بين نظامي تايلز وأوبونتو لكي تفهمن المجموعة بشكل أفضل كيفية استخدامها في عملية "إعادة الضبط" الخاصة بهن.

١٠. إختتمن الجلسة بمناقشة كيف يمكن أن تكون عملية إعادة الضبط بواسطة تايلز أو أوبونتو خياراً لفتح "صفحة جديدة" على حواسيب المشاركين في حال التعرّض لهجوم برمجيات خبيثة أو أي فقدان آخر للسيطرة، ولكن إحرصن أيضاً على ذكر أنواع أخرى

من الهجمات التي لا ينفع فيها هذا الحلّ بشكلٍ فعال، كالعنف على الإنترنت.

المراجع

- <https://tails.boum.org/>
- <http://www.ubuntu.com>